Cloud Computing Security Issues and its Solution: A Review

Randeep Kaur
M.Tech Scholar, Department of CE
Punjabi University, Patiala, INDIA.
Email Id: ryna.sidhu@gmail.com

Jagroop Kaur
Assistant Professor, Department of CE
Punjabi University, Patiala, INDIA
Email Id: jagroop_80@rediffmail.com

Abstract* – Cloud Computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. As information exchange plays an important role in today's life, information security becomes more important. This paper is focused on the security issues of cloud computing and techniques to overcome the data privacy issue. Before analyzing the security issues, the definition of cloud computing and brief discussion to under cloud computing is presented, then it explores the cloud security issues and problem faced by cloud service provider. Thus , defining the Pixel key pattern and Image Steganography techniques that will be used to overcome the problem of data security.

Keywords-Cloud Computing, Cloud Security, Security issues, Image steganography, Pixel key pattern.

NOMENCLATURE

Software as a service (SaaS) , Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

I. INTRODUCTION

Internet has been a driving force towards the various technologies that have developed since its inception. Arguably, one of the most discussed among all of them is *Cloud Computing*. Over the last few years, Cloud computing paradigm has witnessed an enormous shift towards its adoption and it has become a trend in the information technology space as it promises significant cost reductions and new business potential to its uses and providers [1]. Cloud computing can be defined as a parallel and distributed computer system consisting of a collection of inter-connected resources based on service-level agreements(SLA) established through negotiation between the service provider and consumers .Single security method cannot solve the cloud computing security problem. So many traditional, new technology and strategies must be used together for protecting the total cloud computing system. To overcome this challenge, we will use image steganography technique with pixel key pattern and proposed simulator CloudSim: an extensible simulation toolkit that supports both system and behavior modeling of Cloud system components such as data centers, virtual machines (VMs) and resource provisioning policies. The remainder of this paper is organized as a brief review of cloud computing, cloud computing security issues, Solution by defining the techniques and Conclusion.

A. Understanding Cloud Computing

Cloud Computing is a flexible, cost-effective, and proven delivery platform for proving business or consumer IT services over the internet. I n a cloud computing environment, the entire data reside over a set of networked resources, enabling the data to be accessed through virtual machines [2]. The definition of cloud computing provided by National Institute of standards and technology(U.S Department of commerce) is as follows:
"Cloud computing is a model for enable infinite network access, conventional usage , on–demand service and scalable resources that are billed on utility basis"[4].
However, Cloud computing presents an added level of risk because essential service are often outsourced to a third party, which makes it harder to maintain data security and privacy[4]. In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. It can deploy, allocate or reallocate resources dynamically with ability to continuously monitor their performance [5]. The advantage of using cloud computing includes:
Reduce hardware and maintenance cost,
Accessibility around the globe, and
Flexibility and highly automated processes wherein the customer need not worry about concerns like software up-gradation [2,3].
There are three main categories of service models of cloud computing: Infrastructure as a Service(IaaS),Platform as a Service(PaaS),and Software as a Service(SaaS). The four deployment models are : public cloud, private cloud ,community cloud and hybrid cloud.

B. Cloud computing Service Models

The cloud service providers three different services based on different capabilities such as Software as a service , Platform as a Service, Infrastructure as a Service.
Software as a Service (SaaS): It consists of software running on the provider's cloud infrastructure, delivered to (multiple) clients(on demand)via a thin Client (eg. Browser) over the internet.

978-9-3805-4416-8/15/$31.00 ©2015 IEEE

- Platform as a Service (PaaS): This gives a developer the flexibility to develop applications on the provider's platform. Entirely virtualized platform that include one or more servers, operating systems and specific applications.
- Infrastructure as a service(IaaS): The service provider owns the equipment and is responsible for housing ,running and maintaining it a service API.

C. Cloud computing Deployment models

The security issues start with the cloud deployment models. Depending on infrastructure ownership, there are four deployment models of cloud computing[6].

- The Public Cloud: Which describe cloud computing in the traditional mainstream sense; resources are dynamically provisioned on a self-service basis over the internet. (e.g Amazon, Google AppEngine)
- The Private Cloud: It defers from the traditional data enter in its predominant use of virtualization. The private cloud is more appealing to enterprises especially in mission and safety critical organizations.
- The Community Cloud: Thus refers to a cloud infrastructure shared by several organization within a specific community. A typical example is the Open Cirrus Cloud Computing Testbed.
- The Hybrid Cloud: It comprises of a combination of any two(or all) of the three models discussed above.

II.SECURITY ISSUES IN CLOUD COMPUTING

A. Components Affecting Cloud Security

There are numerous security issues for cloud computing as it encompasses many technologies including virtualization ,resource allocation ,tractional management, cloud networks, database, Operating systems, concurrency control and memory management. For example, security in cloud network that interconnects the systems in a cloud has to be secure. Virtualization paradigm in cloud computing results in several security concerns[9]. And mapping the virtual machine to the physical machine has to be carried out securely. Concurrency control involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing .Resource allocation and memory management algorithm have to be secure.

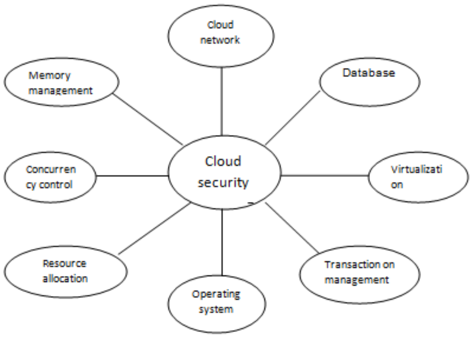

Fig. 1. Components Affecting Cloud Computing

B. Security Issues Faced By Cloud Computing

Cloud allows to achieve the power of computing which beats their own physical domain . it leads to many security problems. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. Cloud computing infrastructure use new technology and services , most which have not been fully evaluated with respect to security. This leads to affects many customers who are sharing the infected cloud. The security issues faced by cloud computing are discussed below[7]:

• *Data Access Control:* Sometimes confidential data can illegally accessed due to the lack of secured data access control. Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system.

• *Data Integrity:* Data integrity comprises the cases, when human errors occurs when data is entered. Errors may occur when data is transmitted from one computer to another, otherwise error can occur from hardware malfunctions ,such as disk crashes.

• *Data loss:*It is a very serious problem in cloud computing. If banking and business transaction ,research and development ideas are all taking place online, unauthorized people will be able to access the information shared.

• *Data Theft;* Cloud Computing uses external data server for cost affective and flexible for operations.

• *Privacy Issues:* Security of the customer personal information is very important in case of cloud computing. Most of the servers are external, so the vendor should make sure that is well secured from other operations.

• *User level issues:* user should make sure that because of its own action, there should not be any loss of data or tampering of data for other users who are using the same cloud.

• *Security issue in Provider level:* Provider should make a good security layer between customer and user. It should make sure that the server is well secure from all the external threats it may across.

III. PROBLEM FORMULATION

Whenever user will send the data to the there are security issues.

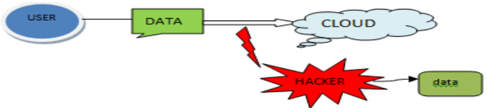

Fig. 2.

The hacker can easily fetch the data which is transfer from user to cloud end. So here is the loss of important business data.

IV.SOLUTION FOR CLOUD COMPUTING SECURITY ISSUES

There are some cloud security solutions, that providers should kept in mind when they delivers their services to cloud service consumer in public cloud solution. Trust between the service provider and the customer is one of the main issue in cloud computing. Service Level Agreement (SLA) is the only legal document between the customer and the service provider, which contain all the agreements between the customer and the service provider, it contains what the service provider is doing and is willing to do. Preserving confidentiality and integrity are the main issues. The main concern over here is the data which is travelled from client end to the cloud server end. The data which is utmost important to the client can be easily hacked by the third party. So we will use the encryption and decryption of data. At the client end, we will encrypt the original data and will send the encrypted data to the cloud server. The cloud server after receiving the encrypted data can decrypt the data; hereby preventing the data loss as shown in fig. 3.The technique for encryption /decryption that we will focusing on is Steganography.

Image Steganography: Steganography is the technique used to hide the information in some other information so that the existence of the secret message cannot be detected easily. In image steganography image is used as the cover information. The cover image is the one in which the secret data is embedded [9]. The image thus obtained by embedding secret data into the cover image is called Stego-image. The secret data is embedded into the image by detecting the edges of the images using pixel key pattern.

Pixel Key Pattern: Edge detection is a tool used in image processing and computer visualization. It is the process which aims at identifying and locating sharp points in an image which are due to change in pixel intensity. The most common algorithm used for edge detection is pixel key pattern. It uses multistage algorithm to detect a wide range of edges in image. The characteristics of this algorithm are: low error rate, edge points be well localized and single response to an edge [8].

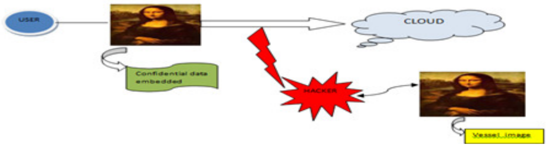

Fig. 3.

TOOL

CloudSim: CloudSim is a toolkit (library) for simulation of Cloud computing scenarios. It provides basic classes for describing data centers, virtual machines, applications, users, computational resources, and policies for the management of diverse parts of the system(e.g., scheduling and provisioning)[10]. These components can be put together for user to evaluate new strategies in utilization of clouds. It can also be used to evaluate efficiency of strategies from different perspectives, from cost/profit to speed up of application execution time. Simulation can be defined as “running a model of software in a model of hardware”.

V.CONCLUSION

Cloud computing by itself is in evolving stage and hence the security implications in it are not complete. It is evident that even the leading cloud providers such as Amazon, Google etc are facing many security challenges and are yet to stabilize. Achieving complete solution for legal issues is still a question. With this level of issues in cloud computing, decisions to adopt cloud computing in an organization could be made only based on the benefits to risk ratio. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the client end and the cloud server end. Main goal of cloud computing is to securely store and transmit the data in cloud.

VI. REFERENCES

[1] L.Wang, Gregor Laszewski, Marcel Kunze, Jie Tao,”Cloud Computing: A Prespective Study”, New Generation Computing-Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008. DOI: 10.1007/s00354-008-0081-5

[2] R. Maggiani, Communication Consultant, Solari communication, “Cloud computing is changing How we communicate”,2009 IEEE International Professional Conference ,IPCC, pp. 1-4,Waikiki,HI,USA, July 19-20,2009. ISB N: 978-1-4244-4357-4.

[3] Harold C. Lin, Shivnath Babu, Jefffrey S. Chase, Sujay S. Parekh,”Automated Control in Cloud Computing: Opportunities and Challenges”, Proc. Of the 1st workshop on Automated control for data centers and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

[4] P.Sharma, S. K. Sood, and S. Kaur,” Security Issues in Cloud Computing”, Proceedings of High Performance Architecture and Grid Computing, Vol. 169, pp. 36-45,20111.DOI:10.1007/978-3-642-22577-5_5.

[5] Thomas W. Shinder,”Security Issues in Cloud Deployment models”, TechNet Articles,Wiki,Microsoft ,Aug,2011.http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud-deployment-models.aspx

[6] Tharam Dillon ,Chen WU and Elizabeth Chang, Cloud Computing :issues and challenges,2010 24th IEEE International Conference on Advanced Information Networking and Applications,150-445X/10.

[7] T.Lindeberg(1998)” Edge Detection and ridge detection with automatic scale selection”, International Journal of Computer Vision, 30,2,pages 117-154.

[8] Manish Mahajan and akashdeep Sharma “Steganography in Coloured Images Using Information Reflector with 2k Correction” 2010 International Journal of Computer Application(0975-8887).

[9] Buyya R,Murshed M. GridSim: A toolkit for modeling and simulation of distributed resources management and scheduling for grid computing. concurrency and computation Practice and Experience 2002; 14(13-15): 1175-1220.

[10] S.Pearson,”taking account of privacy when designing cloud computing services”, CLOUD’ 09 Proc. Of ICSE Workshop on Software Engineering Challenges of Cloud Computing ,pp.44-52,IEEE Computer Society Washington,DC,USA,May 2009.ISBN: 978-1-4244-3713-9.